UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/920,784	08/01/2001	Roberto Fabian Averbuj	010343	5164

23696 7590 12/20/2005

QUALCOMM, INC
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
DERWICH, KRISTIN M	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/920,784	AVERBUJ ET AL.	
	Examiner	Art Unit	
	Kristin Derwich	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-25 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-25 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 29 December 2003 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2/10/03.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-25 are pending.

Claim Rejections - 35 USC § 112

Amendments to the claims are acceptable and the previous rejections are withdrawn in regard to claims 1, 8-14, 16 and 17.

Response to Amendment

Applicant's amendments with respect to previously presented claims 5-7, 15, 18 and 23-25 and amended claims 1-4, 8-14, 16-17 and 19-22 filed September 13, 2005, have been fully considered (MPEP 714.04; 37 CFR 1.111) but are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Arguments

2. Applicant's arguments filed September 13, 2005 have been fully considered but they are not persuasive. Applicant contends that the KASUMI Specification fails to teach the KASUMI algorithm implemented on hardware such as circuits, memory for storing outputs, input muxes, etc. The Examiner respectfully disagrees with Applicant on this point. The KASUMI Specification discloses the KASUMI algorithm being designed to be implemented in hardware (pg. 20). The use of combinational logic and hardware is sufficient to enable one in ordinary skill in the art to implement the algorithm onto hardware.

Due to the reasons stated above, the Examiner maintains rejections with respect to previously presented claims 1-25. The KASUMI Specification teaches the limitations that the

Applicant suggests distinguish from the prior art. Furthermore, the admitted prior art, in combination with The KASUMI Specification, teach the limitations not explicitly disclosed by The KASUMI Specification. Therefore, it is the Examiner's conclusion that previously presented claims 1-25 are not patentably distinct or non-obvious over the prior art of record at present.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-4 and 8-25 are rejected under 35 U.S.C. 102(b) as being anticipated by the KASUMI Specification Version 1.0, 3GPP, 23 December 1999 (hereinafter "the KASUMI Specification).

Regarding claim 1, the KASUMI Specification discloses generating a fractional portion of the KASUMI cipher operably coupled to a calculation controller for sequencing eight rounds to produce a KASUMI output (see paragraph 3.2).

Regarding claims 2, 4, 14,15,18, and 23-25, the KASUMI Specification discloses a subkey generator for each of eight rounds based on the 128-bit key, using shift registers, masking, and rotating (see paragraph 4.6).

Regarding claims 3 and 8, the KASUMI Specification discloses performing KASUMI with a key comprising generating a fractional portion of the KASUMI cipher, configurable for

calculation of even and odd rounds for eight rounds (see paragraph 4.1), storing the output of the KASUMI round and providing input to the KASUMI round, the input being selected during the first round and the contents of the memory being selected during subsequent rounds (see paragraph 4.1; page 24, function Kasumi), and each round receiving an input and producing an output, operable with a partial round calculator, storing an intermediate value from the partial round calculator, and selecting between the input and the contents of the memory for delivery to the partial round calculator (see paragraph 4.1; page 24, function Kasumi).

Regarding claim 9, the KASUMI Specification discloses A KASUMI round for receiving a 64-bit input and producing a 64-bit output comprising: an FO function, an FL function, an XOR gate, a first register, a second register for receiving the outputg of the XOR gate, the output being concatenated with the output of the first register to produce the 64-bit output; a first input mux for selecting between the upper half of the 64-bit input and the output of the second register under control of an input select signal, the output being received at the first register; a second input mux for selecting between the lower half of the 64-bit input and the output of the first register under control of the input select signal, the output being delivered as the second operand to the XOR gate; a first datapath mux, the output of which is delivered to the FL function, for selecting between the output of the first input mux and the output of the FO function under control of a data flow signal; a second datapath mux, the output of which is delivered to the FO function, for selecting between the output of the FL function and the output of the first register under control of the data flow signal; and a third datapath mux, the output of which is delivered as the first operand to the XOR gate, for selecting between the output of the FL function and the FO function under control of the data flow signal (see paragraphs 4.1-4.4).

Regarding claims 10,11,19, and 20, the KASUMI Specification discloses an FO function which receives an input, produces an output, uses XOR gates, calculates partial results and stores intermediate values, and selects between the input and the stored result (see paragraph 4.3; page 23, function FO).

Regarding claims 12,13, 21, and 22, the KASUMI Specification discloses an Fl function which receives an input, produces an output, uses XOR gates, muxes, and S9 and S7 functions, calculates partial results and stores intermediate values, and selects between the input and the stored result (see paragraph 4.4, page 22, function Fl).

Regarding claim 16, the KASUMI Specification discloses eight rounds of KASUMI ciphering, calculating step in which the input is selected during the first round and the stored result is selected during subsequent rounds, calculating and storing a partial result, and delivering the stored result as output (see paragraph 4.1).

Regarding claim 17, the KASUMI Specification discloses performing the FL function then the FO function, and XORing the output with the lower half of the input or stored result when the round is odd; and performing the FO function then the FL function, and XORing the output with the lower half of the input or stored result when the round is even; and delivering as the partial result the output of the XORing step concatenated with the upper half of the input or stored result (see paragraphs 3.2 and 4.1).

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 5-7 are rejected under the KASUMI Specification, as established above, in view of admitted prior art. The preparers of the KASUMI Specification, the 3GPP Task Force (see page 3), did not state the application of the KASUMI cipher. However, Applicants admit that the 3GPP intended for the KASUMI cipher to be used in an access point (base station), an access terminal (mobile station), and operable in a W-CDMA system (see paragraphs 1003,1004,1006, and 1007). In light of the intended use of the KASUMI algorithm, it would have been obvious to use it operable in a W-CDMA system in an access terminal and access point.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Lee et al., U.S. Patent No. 6,314,186 disclose methods where an encryption algorithm is implemented on hardware.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kristin Derwich
Examiner
Art Unit 2132

KMD

KMD

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100